

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2001-521261

(P2001-521261A)

(43) 公表日 平成13年11月6日 (2001.11.6)

(51) Int. Cl. ⁷	識別記号	F I	テームコード* (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H, 5 C 0 5 3
			D, 5 D 0 4 4
H 0 4 N 5/91		H 0 4 N 5/91	P
5/92		5/92	H

審査請求 未請求 予備審査請求 有 (全 47 頁)

- (21) 出願番号 特願2000-518385(P2000-518385)
 (86) (22) 出願日 平成10年10月19日 (1998.10.19)
 (85) 翻訳文提出日 平成12年4月24日 (2000.4.24)
 (86) 国際出願番号 PCT/US 98/22126
 (87) 国際公開番号 WO 99/22372
 (87) 国際公開日 平成11年5月6日 (1999.5.6)
 (31) 優先権主張番号 08/957,051
 (32) 優先日 平成9年10月24日 (1997.10.24)
 (33) 優先権主張国 米国 (US)

- (71) 出願人 ソニー エレクトロニクス インク
 アメリカ合衆国 ニュージャージー州
 07656 パークリッジ ソニー ドライブ
 1
 (72) 発明者 小室 輝芳
 日本国神奈川県川崎市宮前区鷺沼3-11-
 130-101
 (72) 発明者 大澤 義知
 日本国神奈川県横浜市長青区美しが丘1-
 10-2-502
 (74) 代理人 弁理士 小池 晃 (外2名)

最終頁に続く

(54) 【発明の名称】 伝送システム及び伝送方法

(57) 【要約】

暗号モード識別子 (EMI) を用いて情報を伝送する伝送方法及び伝送システムに関する。本発明は、(例えば、音声/画像作品を示す) データが、ソース装置からシンク装置 (受信局) に伝送される際に用いられる複数の保護通信モードを提供する。第1の保護モードであるEMIモードAでは、伝送される情報が、作品全体に渡ってコピーが許可されない。これは、最も高レベルのコピー禁止である。第2の保護モードであるEMIモードBでは、伝送される情報が、シンク装置によって一世代コピーのみを許可される。第3の保護モードでは、暗号化が行われず、自由なコピーが可能である。モードA及びモードBのいずれの保護モードが選択されるかによって、ソース装置は伝送情報を暗号化する際に異なる暗号化処理を用いる。更に、モードA及びモードBのいずれの保護モードが選択されるかによって、シンク装置は伝送情報を暗号解読する際に異なる暗号解読処理を用いる。本発明は、ソース装置と、バケットヘッダからコピー制御情報を抽出する能力を備えていないビットストリーム記録装置との間での伝送に特に有効である。各伝送

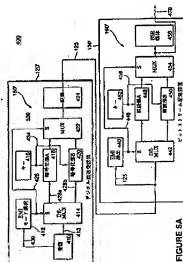


FIGURE 5A

【特許請求の範囲】

【請求項1】 情報を伝送する伝送システムにおいて、

暗号化モード識別子（EMI）コードが第1のモードを示すときに、情報パケットのデータを暗号化する第1の暗号回路と、上記EMIコードが第2のモードを示すときに、上記情報パケットのデータを暗号化する第2の暗号回路とを有し、上記EMIコードをエンコードして上記情報パケットにして、上記情報パケットを通信インタフェースを介して伝送するソース装置と、

上記通信パケットから上記EMIコードを抽出する抽出回路と、上記EMIコードが上記第2のモードであることを示す上記抽出回路に反応して、上記情報パケットのデータを暗号解読する第2の暗号解読回路とを有し、上記通信インタフェースから上記情報パケットを受信するシンク装置とを備え、

上記第1のモードは、上記情報パケットが上記シンク装置によって再生されないことを示すコピー禁止モードであり、上記第2のモードは、上記情報パケットが上記シンク装置によって1回以上再生されないことを示す1回コピー許可モードであることを特徴とする伝送システム。

【請求項2】 上記シンク装置は、更に、上記EMIコードが上記第1のモードであることを示す上記抽出回路に反応して、上記情報パケットのデータを暗号解読する第1の暗号解読回路を備えることを特徴とする請求項1記載の伝送システム。

【請求項3】 上記第1の暗号回路と、上記第2の暗号回路と、第1の暗号解読回路と、第2の暗号解読回路は接続され、1個の等しい暗号キーを受信することを特徴とする請求項2記載の伝送システム。

【請求項4】 情報を伝送する伝送システムにおいて、

暗号化モード識別子（EMI）コードが第1のモードを示すときに、第1のキーに基づいて情報パケットのデータを暗号化する共通の暗号回路を有し、上記EMIコードをエンコードして上記情報パケットにして、上記情報パケットを通信インタフェースを介して伝送するソース装置と、

上記通信パケットから上記EMIコードを抽出する抽出回路と、上記EMIコードが上記第2のモードであることを示す上記抽出回路に反応して、上記第2の

キーを用いて上記情報パケットのデータを暗号解読する共通の暗号解読回路とを有し、上記通信インタフェースから上記情報パケットを受信するシンク装置とを備え、

上記第1のモードは、上記情報パケットが上記シンク装置によって再生されないことを示すコピー禁止モードであり、上記第2のモードは、上記情報パケットが上記シンク装置によって1回以上再生されないことを示す1回コピー許可モードであることを特徴とする伝送システム。

【請求項5】 上記シンク装置はビットストリーム記録装置であり、上記シンク装置は、更に、上記EMIコードが上記第2のモードであるときに上記情報パケットを記録する記録媒体を備え、上記記録媒体に記録された後、上記シンク装置によって、上記情報パケットの上記EMIコードが上記第2のモードに変換されることを特徴とする請求項1又は4記載の伝送システム。

【請求項6】 上記シンク装置の上記共通の暗号解読回路は、また、上記EMIコードが上記第1のモードであることを示す上記抽出回路に反応して、上記第1のキーを用いて上記情報パケットのデータを暗号解読するためのものであることを特徴とする請求項4記載の伝送システム。

【請求項7】 上記通信インタフェースは、IEEE1394通信規格に準拠したシリアル通信インタフェースであり、上記情報パケットはデジタルの情報パケットであることを特徴とする請求項2又は6記載の伝送システム。

【請求項8】 上記ソース装置は放送受信装置であり、更に、コピー制御情報(CCI)を用いてエンコードされた情報パケットを受信し、コピー保護コードを抽出する受信回路を備え、上記シンク装置は、CCI情報を用いてエンコードされた情報パケットを処理することができないことを特徴とする請求項2又は6記載の伝送システム。

【請求項9】 上記情報パケットは、1まとまりのデジタルの音声／画像プログラムを示すことを特徴とする請求項2又は6記載の伝送システム。

【請求項10】 上記ソース装置及び上記シンク装置は、それぞれ、共通のキーに基づいて上記第1のキーを生成する第1のハッシュ回路と、上記共通のキーに基づいて上記第2のキーを生成する第2のハッシュ回路とを

備え、

上記情報パケットが上記シンク装置によって受信される前に、上記共通のキーが、上記シンク装置及び上記ソース装置間で伝送されることを特徴とする請求項6記載の伝送システム。

【請求項11】 コピー保護モードを有し、情報を伝送する伝送方法において、

ソース装置が、コピー保護モードを有する情報パケットを受信するステップと

上記ソース装置が、上記コピー保護モードに従って、暗号化モード識別子（EMI）コードを上記情報パケットのヘッダに格納するステップと、

上記ソース装置が、上記EMIコードが第1のモードであるときに第1の暗号化構造を用いて上記情報パケットのデータを暗号化するステップと、

上記ソース装置が、上記EMIコードが第2のモードであるときに第2の暗号化構造を用いて上記情報パケットのデータを暗号化するステップと、

上記ソース装置が、上記EMIコードが第3のモードであるときに上記情報パケットのデータを暗号化しないステップと、

上記第1のモードは、上記情報パケットがシンク装置によって再生されないことを示すコピー禁止モードであり、上記第2のモードは、上記情報パケットが上記シンク装置によって1回以上再生されないことを示す1回コピー許可モードであり、上記第3のモードは、上記情報パケットが上記シンク装置によって自由に再生されることを示す無制限モードであり、上記ソース装置が、上記シンク装置に上記情報パケットを伝送するステップとを有する伝送方法。

【請求項12】 更に、上記シンク装置が、上記情報パケットを受信して、上記EMIコードを抽出するステップと、

上記シンク装置が、上記EMIコードが上記第1のモードであるときに第1の暗号解読構造を用いて上記情報パケットのデータを暗号解読するステップと、

上記シンク装置が、上記EMIコードが上記第2のモードであるときに第2の暗号解読構造を用いて上記情報パケットのデータを暗号解読するステップと、

上記シンク装置が、上記EMIコードが上記第3のモードであるときに上記情

報パケットのデータを暗号解読しないステップとを有する請求項11項記載の伝送方法。

【請求項13】 更に、上記シンク装置が、上記EMIコードを上記第2のモードから上記第1のモードに変換して、新しいEMIコードを上記情報パケットに格納するステップと、

上記シンク装置が、上記情報パケットを記録するステップとを有する請求項12項記載の伝送方法。

【請求項14】 ソース装置が、コピー保護モードを有する情報パケットを受信する上記ステップは、上記ソース装置が、エンコードされたCCI情報を有する情報パケットを変換して、上記コピー保護モードを抽出するステップを有することを特徴とする請求項12項記載の伝送方法。

【請求項15】 上記情報パケットは、1まとまりの音声／画像プログラムのデジタル表現であることを特徴とする請求項12項記載の伝送方法。

【請求項16】 上記ソース装置は放送受信装置であり、上記シンク装置はビットストリーム記録装置であることを特徴とする請求項12項記載の伝送方法。

【発明の詳細な説明】

【0001】

発明の分野

本発明は、伝送システム及び伝送方法を開示する。一実施の形態において、暗号化モード識別子(encryption mode indicator)を用いて情報を伝送する伝送方法及び伝送システムを開示する。本発明は、情報通信システムの分野に関する。より詳しくは、本発明は、音声／画像作品を表す情報の安全な(secure)通信モードの分野に関する。

【0002】

関連技術

近年、デジタルインタフェースを用いて複数の音声／画像(AV)機器を接続し、AV情報(例えば、映画、歌等のAV作品を表す情報)を、情報源(例えば、ビデオディスクプレーヤ又はビデオテープレコーダ)から情報表示装置(例えば、テレビジョン受像機又はモニタ受像機)又は情報シンク装置(information sink device)に伝送する技術がある。この技術の発達によって、AV機器にIEEE1394シリアル通信規格が採用されている。IEEE1394シリアル通信規格において、情報は、一定のヘッダ情報及びデータセクションを有するデジタルパケットで伝送される。

【0003】

伝送されるAVデジタル情報(例えば、映画を表す情報)は、通常、著作権によって保護されており、認可されていないユーザがその情報を見たり、そのAV作品を不当に再生することは禁止されている。不当なコピーを防止するために、AV情報は、コピー制御情報(Copy Control Information:CCI)ビットと呼ばれるエンコードされたコピー制御情報と共に伝送される。CCIビットは、コピー世代管理方式(Copy Generation Management System:CGMS)ビットとも呼ばれる。

【0004】

エンコードされたCCIコードは、2ビットからなり、「00」、「10」、及び「11」は、それぞれ「コピーの無制限許可」、「一代代コピーの許可」、

及び「コピーの禁止」を示している。「01」ビットコードは使用されていない。特定のAV情報にどのCCIビットが加えられるかは、AV情報（例えばムービングピクチャエキスパートグループMPEG、デジタルビデオDV及びオーディオデータ）の種類によって規定されている。これらのCCIビットは、AV情報を構成するデータパケットのデータ部中に加えられており、下流の装置によるAV情報の使用を制御している。

【0005】

データの記録毎に、記録装置はパケットのAV情報に加えられているCCIコードを調べ、CCIコードがコピーの禁止を示しているときには、AV情報を記録することを禁止する。CCIコードが一代コピーを許可しているときには、CCIコードはコピー禁止モードに変えられるとともに、AV情報は1回記録媒体に記録される。すなわち、元のデータから許可されているコピー世代は制限される。

【0006】

更に、コピー世代の制限方式を強化するために、CCIコードが暗号化されて情報のデータ部に加えられ、その情報を解読する権利は、そのコピー世代の制限方式に適合する装置のみを製造するように契約している製造者に与えられるという方法が用いられている。記録装置が、AV情報中に暗号化されているCCIコードを調べるか又は変えるためには、その装置にマイクロコンピュータを搭載するか、又はその処理のための専用のハードウェアを設ける必要がある。多くの種類のAV情報と適合させるためには、必要とされる暗号解読の回路は比較的複雑となり、装置のコストも増加する。

【0007】

例えば、ビットストリーム記録(BSR)装置のような安価な記録装置を製造するために、上述した専用のハードウェアが取り除かれた装置はAV情報中のCCIコードを読むことができないことが考えられる。この安価なBSR装置において、AVパケット中に、コピー保護の情報を格納するための特定のフィールドを設けることが考えられている。FIG. 1は、IEEE1394規格に基づくヘッダ部12と、パケット(CIP)ヘッダ部14と、データフィールド部16

とを有する従来の情報パケットのフィールドを示している。このデータパケットはアイソクロナスパケットである。CIPヘッダ部14には、特化されたビットストリームコピー制御情報(BCI)フィールド20が含まれている。BCIフィールド20は、AV情報がBSR装置に伝送されるときに用いられるコピー保護の情報を有している。データ部16は暗号化されたデータを有することではできるが、CIPヘッダ部14は、通常、BSRの限られた性能に適応するように暗号化せずに伝送する。

【0008】

このパケット10に対して、BSR装置はパケットヘッダ14のBCIフィールド20を調べて、パケットがコピー禁止を示しているときは記録をせず、パケットが一世代コピー許可又はコピー無制限許可を示しているときはデータを記録することができる。許可されると、パケットの情報は、パケットヘッダ14に格納されているBCIコード20とともに、BSR装置によって記録される。元のパケットヘッダが一世代コピー許可を示しているときは、記録されている情報が再生されて、BSR装置からIEEE1394バスに供給された後、再生されたBCIコードはコピー禁止を示す(既に1回コピーされたためである)。しかしながら、元のBCIコードが無制限コピーを示しているときは、同じBCIコードは格納されて伝送される。

【0009】

FIG. 2は、上述したコピー保護が不当な装置34によって妨害される可能性があるシステム30を示している。FIG. 2に示すように、ソース装置32は、BSR装置であるシンク装置36に情報を伝送する。妨害装置34が、この通信路(38aと38b)の間に位置している。パケットが送信装置32からシンク装置36に伝送されている間に、パケットヘッダ14のBCIコード20は、妨害装置36によって妨害される。例えば、送信装置32は、コピー禁止を示すビットコード「11」を有するBCIコード20を送信するが、これは、送信の際に、(妨害装置34によって)一世代コピー許可を示すビットコード「10」に不正に変えられるか、又は、無制限コピーを示すビットコード「00」に変えられることもある。このパケットを受信すると、パケットヘッダ14のBCI

コードは、一世代コピー又は無制限コピーを許可しているため、BSR36は、そのデータが本当はコピーを禁止しているという事実を通知されずに、そのパケットの情報を記録する。すなわち、コピー世代は制御されていない。

【0010】

したがって、パケットの情報が、妨害装置に妨害されることなく、ソース装置から知的でない装置に伝送されるコピー保護システムが必要である。更に、パケットの情報が、妨害装置に妨害されることなく、ソース装置からBSR装置に伝送されるコピー保護システムが必要である。さらに、伝送の際に、コピー保護モードの情報が変えられることなく、シンク装置に対して使用可能な値を供給する方式が必要である。本発明は、このような優れた特徴を提供するものである。先に詳細に述べていない本発明のこれら及び他の利点は、ここに示す本発明の説明において明らかになる。

【0011】

発明の開示

暗号化モード識別子(EMI)を用いて情報を伝送する伝送方法及び伝送システムを説明する。本発明は、例えば、著作権を有する音声/画像作品の伝送のように、コピー保護情報が装置間で伝送される用途において有効である。本発明は、伝送が個々の情報パケットで行われるIEEE1394シリアル通信規格において用いることができる。

【0012】

本発明は、(例えば、音声/画像作品を示す)データが、ソース装置からシンク装置(受信局)に伝送される際に用いられる複数の保護通信モードを提供する。第1の保護モードであるEMIモードAでは、伝送される情報が、作品全体に渡ってコピーが許可されない。これは、最も高レベルのコピー禁止である。第2の保護モードであるEMIモードBでは、伝送される情報が、シンク装置によって一世代コピーのみを許可される。第3の保護モードでは、暗号化が行われず、自由なコピーが可能である。モードA及びモードBのいずれの保護モードが選択されるかによって、ソース装置は伝送情報を暗号化する際に異なる暗号化処理を用いる。更に、モードA及びモードBのいずれの保護モードが選択されるかによ

って、シンク装置は伝送情報を暗号解読する際に異なる暗号解読処理を用いる。
すなわち、EMIコードは、(1)伝送情報のコピー保護コードと、(2)使用
される暗号化処理の両方を示している。

【0013】

本発明は、ソース装置と、パケットヘッダからコピー制御情報を抽出する能力
を備えていないビットストリーム記録装置との間での伝送に特に有効である。各
伝送モードによって異なる暗号化処理を行うことによって、選択される暗号解読
処理は、行われた暗号化処理とは異なるため、ソース装置とシンク装置との間に
位置してEMIコードを変更する不当な装置は、音声／画像作品をその後再生し
たり記録したりすることはできない。

【0014】

本発明の一実施の形態では、1つの暗号化処理が用いられるが、データを暗号
解読するのに、2つの異なる暗号キー（キーA及びキーB）が用いられる。この
実施の形態では、パケットヘッダに格納されるEMIコードに対応する暗号キー
を用いて、情報が暗号化される。EMIコードがモードAからモードBに変換さ
れるとき、シンク装置は、キーBを用いて伝送信号を暗号解読する。この例では
、暗号化はキーAによって行われているため、シンク装置によって得られるもの
は、無意味な数字である。シンク装置において再生されるものは、そのシンク装
置によって記録されたとしても、全く元のAV情報ではなく、無意味なものとな
る。

【0015】

発明を実施するための最良の形態

以下に示す、ソース装置とビットストリーム記録（BSR）装置との間におけ
るコピー保護の情報の安全な伝送を提供するための本発明を適用した方法及び装
置の詳細な説明では、本発明の十分な理解のために、多数の具体的な説明を行う
。しかし、本発明は、これらの具体的な説明の範囲内に限定されるものではなく
、同等な物においても実行されうるということは、当該技術分野の専門家によつ
て認識される。他の例では、本発明の要点を不必要に曖昧にしないために、周知
の方法、工程、構成要素、及び回路は、詳細に説明しないこととする。

【 0 0 1 6 】

本発明では、パケットがソース装置から伝送されるときに、A Vパケットの情報が暗号化され、使用される暗号モード又は暗号処理は、暗号化モード識別子 (E M I) コードに従って変えられる。本発明のE M Iコードは、コピー禁止モード、一世代コピー許可モード、無制限モードという3つの条件を表している。「一世代コピー」という用語は、元の作品は、それから多数のコピーを作ることは許可されているが、元の作品のコピー (例えば、シンク装置に送られたもの) は、1回のみコピーできるということを意味している。選択された暗号モードを示すE M I情報は、パケットヘッダに格納される。E M I情報が受信側で傍受されると、シンク (受信) 装置は、本当の暗号モードとは異なる暗号モードで暗号を解読することになるため、パケットから正しいA V情報を取得することができない。一実施の形態では、暗号モードは、暗号処理及び暗号キーを有しており、レジスタの初期値を有することもできる。

【 0 0 1 7 】

更に、送信装置及びシンク装置が、情報のパケットに加えられているE M I情報を理解できるかどうかによって、個々の通信は、異なる暗号モードを用いるように分類され、送信装置及びシンク装置が、他方の装置を認識できるようにする。

【 0 0 1 8 】

E M I 保護通信モード

FIG. 3は、本発明を適用した多数の装置構成要素を含む具体的なシステム100を示すブロック図である。システム100は、例えば、放送チャンネル115を介して、デジタル番組を表すデジタルA V情報を通信することができる無線送信機110を含んでいる。一実施の形態では、送信機110は、衛星放送の送信機であってもよい。他の実施の形態では、伝送線115は、無線ではなく、有線である。この場合、送信機110は、ケーブル又は有料テレビジョン放送会社の地上配備の送信機である。

【 0 0 1 9 】

システム100は、また、デジタル放送受信機120を含んでいる。このデジ

タル放送受信機120は、セットトップボックス(STB)とも呼ばれる。ここでは、デジタル放送受信機120は、ソース装置120と呼ばれる。ソース装置120は、本発明を適用したEMI回路150を備えており、後述するように、多数のEMI通信モードをサポートする。EMI回路150は、各EMI暗号モードによって異なる暗号構造を用いる。ソース装置120は、知的な装置であり、コピー保護の規格に準拠した処理を行う専用の回路を備える。例えば、ソース装置120は、伝送線115を介してデジタル番組を受信し、このデジタル番組は、コピー制御情報(CCI情報)を用いてエンコードされる。

【0020】

FIG. 3のシステム100は、また、シンク装置130を含んでおり、この具体例では、シンク装置130はビットストリーム記録(BSR)装置130であり、シリアルインタフェース125を介してソース装置120に接続されている。シンク装置130は、BSR装置として示されているが、FIG. 8に示すどの受信装置でもよい。多くの場合、シンク装置130は、コストを抑えるために、比較的簡易な装置であり、全てのコピー保護の規格に準拠した処理を行うのに必要な全種類の専用の回路を備えているわけではない。例えば、シンク装置130は、CCIコードのAV情報をデコードする能力を持っていない。しかしながら、シンク装置130は、本発明を適用したEMI回路160を備えている。EMI回路160は、EMIコードに従って暗号化されたAV情報のバケットを暗号解読(復号)する能力を有している。シンク装置130は、シリアルインタフェース125を介してソース装置120からのデジタル情報を受信するために、ソース装置120に接続されている。デジタル情報は、IEEE1394通信規格を用い、シリアルインタフェース125を介して伝送される。更に、この情報はヘッダ部のヘッダ情報及びデータ部のAV情報(例えばデータ)を有するデジタルデータバケットの状態で伝送される。

【0021】

後述するが、FIG. 8のEMI回路150及び160は、それぞれが2つの暗号回路を備え、シリアルインタフェース125を介して伝送される情報が、少なくとも2つの異なる暗号構造A及びBのもとでエンコードされるようになって

いる。一実施の形態では、EMI回路160は、2つの暗号回路を備えており、モードA又はモードBのいずれかの暗号構造で、シリアルインタフェース125を介して受信した情報を（許可されれば）暗号解読できるようになっている。本発明では、BCIコードを用いるのではなく、シリアルインタフェース125を通るデータパケットに入っているEMIコードを用いる。EMIコードは、コピー保護モードを決定するだけでなく、パケットのデータ部で用いられる暗号モードをも決定する。すなわち、シンク装置130中のEMI回路160は、EMIモードを用いて適切な暗号解読構成を選択し、シリアルインタフェース125を介して受信された情報を暗号解読する。もし、本発明を適用したEMIコードが、シンク装置130とソース装置120との間で、（例えば、中間の妨害装置によって）改ざんされた場合、本発明を適用したEMI回路160は、不適切な暗号解読モードを選択してしまう。この具体例では、元の情報は、シンク装置130によって受信されない。

【0022】

シリアルインタフェース125を介して伝送されるAV情報のパケットには、3つの種類がある。これらは、コピー許可情報と、1回コピー情報と、コピー禁止情報である。本発明では、この3種類の情報コピー保護は、異なる保護レベルを有している。コピー保護が各パケットに施される状態は、EMIモードと呼ばれる。後述するように、本発明では、EMIモードは、そのEMIモードが施されたAV情報に適用される暗号化モードをも示している。

【0023】

本発明を適用した暗号すなわちEMIモードを以下に説明する。EMIモードAは、パケットのデータのコピーが禁止されていることを示す際に用いられる。このEMIモードAにおいては、AV情報は再生装置（例えば、テレビジョン受像機又はモニタ受像機）においてのみ再生可能だが、AV情報が記録されることは許可されていない。EMIモードBは、AV情報のコピー（例えば、記録）が1回のみ可能で一代コピーが許可されていることを示す際に用いられる。このEMIモードBは、一代コピー許可モードとも呼ばれる。EMIモードOは、AV情報にコピー保護がなく、コピーの制限がないときに用いられる。このEMI

1モードOは、無制限モードとも呼ばれる。説明を簡潔にするために、本発明では、EMIモードOでは、暗号化が行われない。AV情報が、n回のコピー（ $n > 1$ ）を許可するコピー制御状態にあるとき、それぞれのn回のコピーに対応するモードを定義することによって、コピー回数を増やすことができる。

【0024】

EMIモードは、多数の周知のエンコード技術を用いて表すことができ、少なくとも2ビットを有するレジスタを用いて示すことができる。本発明の一実施の形態では、2ビットのレジスタが用いられる。表1は、各EMIモードにおける具体的な符号化の数値を示している。なお、表1において選択されている符号化の数値は一例であり、3種類の固有の数値の一集ならんでも用いることができる。

【0025】

【表1】

EMIモード	2ビットの数値	説明
モードA	11	コピー禁止
モードB	10	1回コピー
モードO	00	コピー無制限
保留	01	

【0026】

シリアルインタフェース125を介して受信されるAV情報は、多様なプログラムを含んでいると考えられる。各プログラムは、それ固有の保護レベルを有している。この場合、コピー禁止ストリーム（コード11）は、少なくとも1個のコピー禁止プログラムを含むストリームである。1回コピーストリーム（コード10）は、コピー禁止プログラムを含まず、少なくとも1個の1回コピープログラムを含むストリームである。ビットストリーム記録（BSR）装置であるシンク装置130（FIG. 3）の具体例においては、シンク装置130は、EMIモードB（又はEMIモードO）において受信されるAV情報のみを記録するこ

とができ、EMIモードAにおいて受信されるAV情報のみを通過させる（拒否する）ことができる。

【0027】

FIG. 4は、(FIG. 3における)ソース装置120からシンク装置130に送信される本発明を適用した典型的な情報パケット200を構成するフィールドを示している。一実施の形態において、FIG. 4の情報パケット200は、IEEE1394通信規格に準拠しているため、この情報パケット200は、IEEE1394のヘッダ部230を含んでいる。このヘッダ部230は、data_lengthフィールドと、tagフィールドと、channelフィールドと、tcodeフィールドと、syフィールドとを含んでいる。ヘッダ部230は、周知のIEEE1394通信規格に準拠しており、tagフィールド及びtcodeフィールド以外のフィールドは、この規格において定義されている。tagフィールドは、データフィールドがCIPヘッダ部240から始めることを示している。tcodeフィールドは、2個の所定の値のうちの1個の値である。データストリームは、1つの1394アインクロナスチャンネルにおける情報のストリームを意味している。

【0028】

情報パケット200は、また、CIPヘッダ部240を含んでいる。本発明においては、CIPヘッダ部240は、一実施の形態において、2ビット分の幅を有し、表1で定義されるようなEMIモードの値を有しているEMIフィールド210を含んでいる。EMIモードの値は、データフィールド250におけるデータ部220に対応した特定の保護通信モードに相当する。後述するように、EMIフィールド210において示されるEMIモードは、(1)選択された特定の保護通信モード（例えば、モードA、モードB又はモードO）及び(2)情報パケット200において用いられる暗号化の技術の特定の種類とを示している。本発明では、情報が(FIG. 3の)IEEE1394のシリアルインタフェース125を介して伝送される際に、(EMIモードA又はEMIモードBのとき)情報パケット200のデータ部220は暗号化されるが、ヘッダ部230及びCIPヘッダ部240は暗号化されない。

【 0 0 2 9 】

EMI フィールド 210 中の EMI モードは、1394 のアイソクロナスストリームにおけるデータストリームのコピー制御の状態を示している。本発明を適用したデータストリームは、幾つかの画像及び／又は音声のプログラムからなり、それらはそれぞれ各プログラムに対応した異なるコピー制御情報を有している可能性があると考えられる。例えば、ソース装置から出力された M P E G の伝送ストリームは、いくつかのプログラムを含んでおり、各プログラムのコピー保護は異なるレベルを有している可能性がある。ソース装置は、ストリーム中で最も規制されたプログラムに対して EMI の値を割り当てる。ビットストリーム記録装置は、EMI の値に基づいて、全てのストリームを記録するか否かを決定する。ストリーム中の各プログラムを個々に処理することができ、また、各プログラムに対応したコピー制御情報を解釈することができる別の種類の記録装置を、フォーマット認識記録装置と呼ぶ。フォーマット認識記録装置は、各プログラムに対応したコピー制御情報を参照し、その動作を決定する。

【 0 0 3 0 】

本発明を適用した EMI 回路

FIG. 5A は、ソース装置 120 及びシンク装置 130 を備える本発明を適用したシステム 400 の具体的構成を示すブロック図である。FIG. 5A は、典型的なソース装置 120 の EMI 回路 150 をより詳細に示している。ソース装置 120 は、EMI 回路 150 の他に（説明を明確にするためにここでは示さないが）多数の周知の回路を備える放送受信機と呼ばれるセットトップボックス（STR）装置であってもよい。受信回路 410 は、AV 情報をデータパケットとして受信し、コピー制御情報（CCI）の規格において必要とされる暗号化を行う。その結果は、通信インタフェース 430 を介して出力されるとともに、インタフェース 413 を介してデマルチプレクサ（DEMUX）414 にも供給される。回路 412 は、EMI モード選択回路であり、コピー保護が必要ととき、再生された CCI に応じて、コピー保護情報として EMI モード A か EMI モード B のいずれかを選択する。コピー保護が必要でないとき、インタフェース 413 は、シリアルインタフェース 125 に直接つながり、データパケットの EMI

フィールド210にEMIモードO(コード「00」)が割り当てられる。

[0031]

コピー保護が必要であるとき、EMIモード選択回路412は、信号線426上の信号によってDEMUX414を制御する。EMIモードAが選択されると、インタフェース413からのデータパケットは、暗号化部A418に供給され、暗号化部A418は、暗号キー416及び独自の第1の暗号化技術に従ってデータパケットのデータ部(例えばデータ部220)を暗号化する。暗号化部A418は、また、データパケットのEMIフィールド210中に「11」のコード(EMIモードA)を挿入する。その結果は、信号線426によって制御されるマルチプレクサ(MUX)422に供給される。MUX422は、任意の出力ドライバ424を用い、暗号化部A418から出力信号をシリアルインタフェース125に出力する。EMIモードBが選択されていると、インタフェース413からのデータパケットは、暗号化部B420に供給され、暗号化部B420は、暗号キー416及び独自の第2の暗号化技術に従ってデータパケットのデータ部(例えばデータ部220)を暗号化する。暗号化部B420は、また、データパケットのEMIフィールド210中に「10」のコード(EMIモードB)を挿入する。その結果は、信号線426によって制御されているマルチプレクサ(MUX)422に供給される。MUX422は、任意の出力ドライバ424を用いて、暗号化部B420から出力信号をシリアルインタフェース125に出力する。この実施の形態では、2つの異なる暗号化部が用いられ、2つの暗号化構造を提供する共通の暗号キー416に基づいて暗号化が行われる。後述するように、暗号キー416は、ソース装置-シンク装置間の認証処理の際に確立する。

[0032]

FIG. 5Aのシンク装置130は、EMI回路160の他に(説明を明確にするためにここでは示さないが)多数の周知の回路を備えている。FIG. 5Aのシンク装置130中のEMI回路160は、解読キー452が暗号キー416と一致していることを想定して、暗号化部A418によって行われた暗号化を解読することができる暗号解読部A448と、解読キー452が正しいことを想定して、暗号化部B420によって行われた暗号化を解読することができる暗号解

読部B450とを備えている。データバケットが、シリアルインタフェース125を介してデマルチプレクサ回路(DEMUX)420とEMIモード抽出回路440によって受信される。EMIモード抽出回路440は、供給されたデータバケットからヘッダ情報を抽出し、ヘッダ情報からEMIフィールド210を抽出する。抽出されたEMIモードに応じて、EMIモード抽出回路440は、信号線446上の信号を制御する。EMIモードOが抽出されると、シリアルインタフェース125上のデータバケットは、直接ビットストリーム記録(MSR)媒体456に供給されるか、又は、何ら変更されることなしに信号線470に直接出力される。

[0033]

EMIモード抽出回路440がEMIモードAを抽出すると、シリアルインタフェース125を介して伝送されてきたデータバケットは、DEMUX442を通過して暗号解読部A448に供給され、暗号解読部A448は、(解読キー452を用いて)データバケットのデータ部を暗号解読し、結果を信号線446によって制御されるマルチプレクサ(MUX)454に供給する。MUX454は、暗号解読部A448からのデータバケットを信号線470にのみ出力する。シンク装置130がBSR装置であるとき、EMIコードAのデータバケットを記録することは許可されないため、この場合、BSR媒体456への記録は禁止される。EMIモード抽出回路440がEMIモードBを抽出すると、シリアルインタフェース125を介して伝送されてきたデータバケットは、DEMUX442を通過して暗号解読部B450に供給され、暗号解読部B450は、データバケットのデータ部を暗号解読するとともに、EMIモードをEMIモードAに変え、EMIフィールド210に「11」コードを格納し、結果を信号線446によって制御されるMUX454に供給する。MUX454は、暗号解読部B450のデータバケットを信号線470に出力し、BSR媒体456へのデータバケットの記録を許可し、EMIモードAとする。シンク装置130がBSR装置であるとき、EMIコードBのデータバケットを記録することは1回のみ許可され、このデータバケットは、BSR媒体456に記録される前にEMIモードAに変わる。この実施の形態では、2個の異なる暗号解読部が用いられ、暗号解読は、1

つの解読キー452に基づいている。

【0034】

シンク装置130がビットストリーム記録(BSR)装置であるとき、EMIモードAで暗号化されたデータを記録することは許可されない。したがって、EMIモードAのための暗号解読部Aは、BSR装置では動作しない。FIG. 6Aは、暗号化部Aを備えないビットストリーム記録(BSR)装置130におけるEMI回路665の具体的な構成を示すブロック図である。この実施の形態では、EMIモード抽出回路440は、シリアルインタフェース125においてEMIモードAを検出すると、暗号解読部B450及びBSR媒体456を停止させる。

【0035】

FIG. 5Aのシステム400は、以下に示す方法で、妨害装置がコピー保護を妨害するのを防止する。EMIモードAのデータパケットがシリアルインタフェース125上でEMIモードBのデータパケットに変更されると、シンク装置130は、データを再生しようとする際に不適切な暗号解読部を用いてしまうことになる。再生信号は無意味な情報となってBSR媒体456に記録される。EMIモードA又はEMIモードBのデータパケットがシリアルインタフェース125上でEMIモードOのデータパケットに変更されると、シンク装置130は、暗号解読を行わず、その信号は再生されない。

【0036】

FIG. 5Bは、ソース装置120'及びシンク装置130'を備える本発明を適用したシステム500の具体的な構成を示すブロック図である。FIG. 5Bは、本発明の他の実施の形態における典型的なソース装置120'のEMI回路150'と、典型的なシンク装置130'のEMI回路160'を示している。この実施の形態では、共通の暗号化部及び共通の暗号解読部が用いられているが、それらには、選択されたEMIモードに応じてそれぞれ異なるキー(キーA、キーB)が供給されるため、これにより、2種類の暗号化-暗号解読の構造が実現される。

【0037】

FIG. 5Bのソース装置120'は、EMI回路150'の他に(説明を明確にするためにここでは示さないが)多数の周知の回路を備える放送受信機と呼ばれるセットトップボックス(STB)装置であってもよい。受信回路510は、AV情報をデータパケットとして受信し、コピー制御情報(CCI)の規格において必要とされる暗号化を行う。その結果は、(EMIモード選択回路514に接続する)通信インタフェース512を介して出力されるとともに、インタフェース513にも供給される。回路514は、EMIモード選択回路であり、コピー保護が必要と、再生されたCCIに応じて、コピー保護情報としてEMIモードAかEMIモードBのいずれかを選択する。コピー保護が必要でないとき、インタフェース513は、シリアルインタフェース125に直接つながり、データパケットのEMIフィールド210にEMIモードO(コード「00」)が割り当てられる。

[0038]

コピー保護が必要であるとき、EMIモード選択回路514は、マルチプレクサ(MUX)516の選択線を制御する。共通の暗号キー524は、第1のハッシュ関数を有し、第1の暗号キー(キーA)をその出力として生成するハッシュ回路A520に供給される。また、共通の暗号キー524は、第2のハッシュ関数を有し、第2の暗号キー(キーB)をその出力として生成するハッシュ回路B522に供給される。EMIモードAが選択されると、MUX516は、キーAを選択して、共通の暗号化部518に出力し、共通の暗号化部518は、キーA及び独自の共通の暗号化技術に従ってデータパケットのデータ部(例えばデータ部220)を暗号化する。共通の暗号化部518は、また、データパケットのEMIフィールド210中に「11」のコード(EMIモードA)を挿入する。その結果は、インタフェース530を通過して任意の出力ドライバ526に供給され、出力ドライバ526は、シリアルインタフェース125を介してデータパケットを出力する。

[0039]

EMIモードBが選択されると、FIG. 5BのMUX516は、キーBを選択して、共通の暗号化部518に供給し、共通の暗号化部518は、キーB及び

独自の共通の暗号化技術に従ってデータパケットのデータ部（例えばデータ部220）を暗号化する。共通の暗号化部518は、また、データパケットのEMIフィールド210中に「10」のコード（EMIモードB）を挿入する。その結果は、インタフェース530を通して任意の出力ドライバ526に供給され、出力ドライバ526は、シリアルインタフェース125を介してデータパケットを出力する。この実施の形態では、2個の異なるキー（A及びB）が用いられ、1個の共通の暗号化部518において用いられる暗号化処理を切り換える。後述するように、共通の暗号キー524は、ソース装置-シンク装置間の認証処理の際に確立する。ソース装置120'及びシンク装置130'は、隠れたチャンネルキーKcを共有した後、ワークキーA及びBを共有する。最初に、ソース装置120'は、シンク装置130'に乱数Naを送信する。ソース装置120'及びシンク装置130'は、内部のEMI回路を用いて、以下の式によってワークキー（キーA及びB）を算出する。

$$\text{KeyA} = \text{HKc}(\text{Na} \parallel \text{Ca})$$

$$\text{KeyB} = \text{HKc}(\text{Na} \parallel \text{Cb})$$

ここで、HKcは、チャンネルキーKcを用いてキー化されるハッシュ関数であり、Ca及びCbは、定数であり、ライセンスコードである。

【0040】

EMI回路150'は、1個の暗号化部518しか必要としないため、有利である。2つのハッシュ回路520、522が必要であるが、この回路は、第2の暗号化部を削除することによって削除された回路よりも一般的に規模が小さい。これは、ハッシュ関数をソフトウェアで実行するときに特に当てはまる。与えられたキーに対してハッシュ関数を決定する必要があるのは1回のみであるため、ハッシュ関数はソフトウェアで実行するのが有益である。

【0041】

FIG. 5Bのシンク装置130'は、EMI回路160'の他に（説明を明確にするためにここでは示さないが）多数の周知の回路を備えている。シンク装置130'中のEMI回路160'は、正しい共通のキーが供給されていることを想定して、1個の共通の暗号化部518によって行われた暗号化を解読するこ

とができる1組の共通の暗号解読部544を備えている。データパケットは、シリアルインタフェース125を介してEMIモード抽出回路540によって受信される。EMIモード抽出回路540は、EMIモード抽出回路440と同様に、受信したデータパケットからヘッダ情報を抽出し、ヘッダ情報からEMIフィールド210を抽出する。抽出されたEMIモードに応じて、EMIモード抽出回路540は、MUX542の選択線を制御する。EMIモード抽出回路540によってEMIモードOが抽出されると、シリアルインタフェース125上のデータパケットは、直接ビットストリーム記録(MSR)媒体550に供給されるか、又は、信号線570を介して直接出力される。

【0042】

コピー保護モードが抽出されると、EMIモード抽出回路540は、マルチプレクサ(MUX)542の選択線を制御する。共通の解読キー554は、第1の暗号キー(キーA)を出力として生成する第1のハッシュ関数を有するハッシュ回路A546に供給される。また、共通の解読キー554は、第2の暗号キー(キーB)を出力として生成する、第1のハッシュ関数とは異なる第2のハッシュ関数を有するハッシュ回路B548に供給される。EMIモードAがデータパケットから抽出されると、MUX542は、キーAを選択して共通の暗号解読部544に供給し、共通の暗号解読部544は、キーA及び独自の共通の暗号解読技術に従ってデータパケットのデータ部(例えばデータ部220)を暗号解読する。共通の暗号解読部544は、また、データパケットのEMIフィールド210中に「11」のコード(EMIモードA)を挿入する。その結果は、出力線570のみに出力される。シンク装置130'がBSR装置であるとき、EMIモードAのデータパケットを記録することは許可されないため、この場合、BSR媒体550への記録は禁止される。

【0043】

EMIモード抽出回路540によってEMIモードBが抽出されるとき、FIG. 5BのMUX542は、キーBを選択して、共通の暗号解読部544に供給し、共通の暗号解読部544は、キーB及び独自の共通の暗号解読技術に従ってデータパケットのデータ部(例えばデータ部220)を暗号解読する。共通の時

号解説部544は、また、データパケットのEMIフィールド210中に「11」のコード(EMIモードA)を挿入する。この時点でEMIモードAである結果は、インタフェース552を介してBSR媒体550に供給され、任意に出力線570に出力される。シンク装置130'がBSR装置であるとき、EMIモードBのデータパケットを記録することは1回しか許可されないため、その後、BSR媒体550への記録が行われる前に、このデータパケットはEMIモードAに切り換えられる。この実施の形態では、2個の異なるキー(A及びB)が用いられ、1個の共通の暗号解説部544において用いられる暗号解説処理を切り換える。後述するように、(共通の暗号キー524と同様に)共通の解説キー554は、ソース装置-シンク装置間の認証処理の際に確立する。EMI回路160は、1個の暗号解説部544しか必要としないため、有利である。2つのハッシュ回路546、548が必要であるが、この加えられた回路は、第2の暗号解説部を削除することによって削除された回路よりも一般的に規模が小さい。与えられたキーに対してハッシュ関数を決定する必要があるのは1回のみであるため、ハッシュ関数546、548はソフトウェアで実行するのが有益である。

【0044】

シンク装置130'がビットストリーム記録(BSR)装置であるとき、EMIモードAで暗号化されたデータを記録することは許可されない。したがって、EMIモードAのためのハッシュ回路Aは、BSR装置では動作しない。FIG. 6Bは、ハッシュ回路Aを備えないビットストリーム記録(BSR)装置130'におけるEMI回路670の具体的な構成を示すブロック図である。この実施の形態では、EMIモード抽出回路540は、シリアルインタフェース125においてEMIモードAを検出すると、共通の暗号解説部554及びBSR媒体550を停止させる。

【0045】

FIG. 5Bのシステム500は、以下に示す方法で、妨害装置がコピー保護を妨害するのを防止する。EMIモードAのデータパケットがシリアルインタフェース125上でEMIモードBのデータパケットに変更されると、シンク装置130'は、データを再生しようとする際に不適切な暗号解説キー(キーAとキ

ーBのいずれか)を用いてしまうことになる。再生信号は無意味な情報となってBSR媒体550に記録される。EMIモードA又はEMIモードBのデータパケットがシリアルインタフェース125上でEMIモードOのデータパケットに変更されると、シンク装置130'は、暗号解読を行わず、その信号は再生されない。

【0046】

FIG. 7は、FIG. 5Aのシステム400において実行される本発明を適用した処理を示すフローチャート700である。ステップ710において、シンク装置とソース装置が互いに認識できるように認証処理が行われる。この処理は、様々な所定のライセンス及びサービスキーを用いて行われる。本発明を適用したステップ710においては、様々な種類の周知の認証処理や安全なキー変換処理が用いられてもよい。認証処理が成功すると、特定のコードが変換され、ステップ720に進む。認証処理が失敗すると、ステップ715において、フローチャート700は、AV情報を交換せずに、最初に戻る。

【0047】

FIG. 7のステップ720において、ソース装置120は、特定のコードを用いて、キーを暗号解読するシンク装置130に暗号化されたキーを送信する。この時点で、ソース装置とシンク装置との間で、暗号キー416と解読キー452は確立されており、これらのキーは同じ値を有する。ステップ730において、ソース装置120は、(例えばCCIモードのような)第1のコピー保護モードを有するデータパケットを受信し、このCCIモードを(例えば、コピー禁止、1回コピー、無制限のような)EMIモードに変換する。ステップ740において、EMI回路150は、受信したデータパケットのヘッダに適切なEMIモードを挿入し、EMIモードにおける2つの使用できる暗号化構造のうちの1つを用いてデータパケットのデータ部を暗号化する。その後、このデータパケットは、インタフェース125を介して伝送される。

【0048】

FIG. 7のステップ750において、シンク装置130は、EMI回路160を用いて、EMIモードを抽出し、抽出されたEMIモードに従ってデータパ

ケットを暗号解読する。2つの使用できる暗号化構造のうちの1つは、EMIモードに基づいて用いられる。EMIモードBが受信されたとき、この情報はEMIモードA(全面保護)で記録される。EMIモードAが受信されると、一切の記録が許可されない。ステップ760において、更にデータパケットの処理が必要であるとき、フローチャート700はステップ740に戻り、次のデータパケットを処理する。必要でなければ、フローチャート700は最初に戻る。

[0 0 4 9]

FIG. 5Bの他の実施の形態の処理動作は、上述した処理と似ているが、ここでは、FIG. 5Bにおける異なる暗号化及び暗号解読の構造を提供するために、異なるキーが用いられる。

[0 0 5 0]

本発明を適用した装置の分類

FIG. 8は、本発明を適用した複数の異なる種類の装置を示している。また、FIG. 8に示すのは、各装置によって受信及び送信される(EMIモードによって分類される)AV情報のパケットの種類である。破線の信号線は、EMIモードBのAV情報パケットを表し、実線の信号線は、EMIモードAのAV情報パケットを表している。第1の装置の分類は、装置分類Aである。これらの装置は、それらのパケット情報にEMIコードを加えることができるとともに、CCIデータを受信することができる送信装置を含む。1つの例は、(例えば、CCIフォーマットで)衛星放送を受信し、IEEE1394のバスを介してデータを送信することができるセットトップボックス(STB)120である。FIG. 8に示すように、STB装置120は、EMIモードA又はEMIモードBのいずれかで暗号化されたAV送信パケットを生成することができる。STB装置120は、また、無制限のAV情報を送信することができる。STB装置120は、出力626で示すように、EMIモードBのAV情報を出力し、出力628で示すように、EMIモードAのAV情報を出力する。

[0 0 5 1]

第2の装置の分類は、装置分類Bである。これらの装置は、AV情報パケット中に存在するEMI情報に応じることができる受信又はシンク装置を含む。分類

B の 1 つの例の装置は、フォーマット認識記録装置 630 である。このフォーマット認識記録装置 630 は、いかなる EMI モードで受信した AV 情報パケットを適切に暗号解読し、IEEE1394 規格のフォーマットを用いて AV 情報を記録し、AV 情報に加えられた EMI 情報を記録し、IEEE1394 規格のフォーマットを用いて、再生されたデータを送信することができる。受信した AV 情報が EMI モード B であるとき、それが記録されるときには EMI モード A に変換されて、それ以上のコピーを防止する。フォーマット認識記録装置 630 は、EMI モード A 632 及び EMI モード B 634 で暗号化された AV 情報のパケットを受信することができるが、EMI モード A 636 で暗号化された AV 情報のみを送信することができる。

【 0052 】

第 3 の装置の分類は、装置分類 C である。これらの装置は、(例えば、CCI モードでの) 特定のコピー保護情報を完全に処理するのに必要な専用の回路を備えていないために、このコピー保護情報を完全には処理することができない受信装置を含む。分類 C の 1 つの例は、FIG. 8 のビットストリーム記録 (BSR) 装置 130 である。このビットストリーム記録 (BSR) 装置 130 は、入力 610 を介して EMI モード B で暗号化された AV 情報のみを受信し、入力 615 を介して EMI モード A で暗号化された AV 情報のみを送信することができる。EMI モード B の情報が受信されたとき、BSR 装置 130 は、抽出された EMI コードを用いて EMI モード B で暗号化された情報を暗号解読し、この情報を記録することができる。BSR 装置 130 は、また、AV 情報を再生し、IEEE1394 規格の元で EMI モード A のこの情報を送信することができる。

【 0053 】

第 4 の装置の分類は、装置分類 D である。これらの装置は、情報パケットに加えられた EMI 情報を処理することができる受信装置を含む。分類 D の 1 つの例は、デジタルテレビジョン受像機 620 である。デジタルテレビジョン受像機 620 は、IEEE1394 規格の元で、入力 622 を介して EMI モード B で暗号化された AV 情報及び入力部 624 を介して EMI モード A で暗号化された AV 情報のみを受信することができる。デジタルテレビジョン受像機 620 は、E

M I モード A 又は E M I モード B の A V 情報を暗号解読し、その A V 情報を再生することができる。

【 0 0 5 4 】

暗号化及び暗号解読モードは、ある団体が実現したい機能に従って、その団体によってライセンスが得られる。その団体が表示装置を製造するとき、E M I モード A 及び E M I モード B の暗号解読のライセンスが必要である。その団体が B S R 装置 1 3 0 を製造するとき、E M I モード B の暗号解読及び E M I モード A の暗号化が必要である。後述するように、本発明の一実施の形態において、E M I モード A 及び E M I モード B は、ライセンスキー及びサービスキーと結合されることが可能である。

【 0 0 5 5 】

本発明の一実施の形態におけるサービスの分類の例

本発明の一実施の形態においては、特定の通信サービスがサポートされる。この実施の形態では、使用するサービスの種類によって、また、装置がソース装置かシンク装置かによって、特定の秘密（例えば、キーコード）が定義される。上述した送信装置及び受信装置の分類に従って、データ伝送のサービスの分類を以下に示す。サービス 1 における伝送は、分類 A、B 又は C の送信装置と、分類 A、B 又は C の受信装置とを含む。サービス 2 における伝送は、分類 A、B 又は C の送信装置と、分類 D の受信装置とを含む。サービス 3 における伝送は、分類 D の送信装置と、分類 A、B 又は C の受信装置とを含む。

【 0 0 5 6 】

例えば、サービス 1 の元では、C C I のコピー保護フォーマットを認識するソース装置が、この C C I のフォーマットを認識するシンク装置に A V 情報を送信する（例えば、S T B → 表示装置、又は、S T B → フォーマット認識記録装置）。ソース装置とシンク装置は両方ともコピー保護を有する知的な装置である。サービス 2 の元では、C C I のフォーマットを認識するソース装置が、C C I のフォーマットを認識しないが本発明を適用した E M I コードを認識するシンク装置に A V 情報を伝送する。このシンク装置は、ソース装置と同レベルのコピー保護の機能を有していない。サービス 3 の元では、C C I のフォーマットを認識しない

いソース装置が、CCIのフォーマットを認識するシンク装置にAV情報を送信する(例えば、DVHS→表示装置)。

【 0 0 5 7 】

本発明の一実施の形態では、EMIモードA、B及びサービス1、2、3を用いるための秘密コード(例えば、キーコード)が、上述の符号を付けた個々の分類の装置に与えられる(例えば、ライセンスされる)。認証処理の際に安全なキーの伝送を行うために、その2個の装置によって、キーコードすなわち「秘密」が用いられる。このようにして、上述したような暗号化及び暗号解読に用いられるキーが、ソース及びシンク装置の間で安全に伝送される。

【 0 0 5 8 】

サービス1、2、3では、送信装置と受信装置で異なるキーコードが必要である。例えば、サービス1の送信装置のキーコードは、受信装置のキーコードとは異なる。ここで、キーコードが個々の装置に供給される方法を説明する。FIG. 9の表に示すように、本発明のこの実施の形態では、8個のキーコードが用いられる。装置の分類は、MPEG又はDVのようなデータの種類によって、更に細かくしてもよい。サービスキーとライセンスキーを含む1組が、サービス1、2及び3にそれぞれ割り当てられる。サポートされるサービスに従って、ソース装置はサービスキーを持ち、シンク装置はライセンスキーを持つ。すなわち、サービス1、2及び3は、サービスキー又はライセンスキーによって区別される。

【 0 0 5 9 】

例えば、STB装置120はサービス1、2を送信するため、サービスキー1及び2を有している。DVHS装置130は、サービス2を受信し、サービス3を送信するため、ライセンスキー2及びサービスキー3を有している。各サービスは、そのサービスのグループ内でサブグループに分割されてもよい。ある装置が有すべき機能によって、暗号化モード、サービスキー及びライセンスキーのある組み合わせがその装置に与えられる。例えば、表示装置620の場合は、EMIモードA及びEMIモードBの暗号解読キーとサービス1及び3のためのライセンスキーを有している。STB装置120の場合は、EMIモードA及びE

MIモードBの暗号化キーとサービス1及び2のためのサービスキーを有している。DVHS(BSR)装置130は、EMIモードAの暗号化キーとサービス3のためのサービスキーを有している。

[0060]

FIG. 9に示すように、分類Aの装置は、サービス1及び2の送信装置のキーコードと、EMIモードA及びBのキーコードを必要とし、Secret1T、Secret1T、Secret1T、Secret1T、Secret1T、Secret1T及びSecretBのキーコードが提供される。同様に、分類Bの装置は、サービス1及び3の受信装置とサービス1の送信装置のキーコードと、EMIモードA及びBのキーコードを必要とし、Secret1R、Secret1R、Secret3R、Secret3R、SecretA及びSecretBのキーコードが提供される。分類Cの装置は、サービス1及び3の受信装置のキーコードと、EMIモードA及びBのキーコードを必要とし、Secret1R、Secret1R、Secret3R、Secret3R、SecretA及びSecretBのキーコードが提供される。分類Dの装置は、サービス2の受信装置とサービス3の送信装置のキーコードを必要とし、Secret2R、Secret3T、SecretA及びSecretBのキーコードが提供される。典型的に、送信専用モードAを使用することと、受信専用モードBを使用することが必要である。

[0061]

本発明を適用したサービスキーを用いた動作

以下、分類Aのソース装置から、受信装置として動作する分類Bのシンク装置にデータパケットを送送する処理について説明する。データパケットは、ソース装置からシンク装置に伝送され、シンク装置によって記録される。

[0062]

送信側のソース装置は、データキーとしてKseedを生成し、データパケットを暗号化する。サービス1の送信装置及び受信装置のための秘密コードSecret1T及びSecret1Rを用いて、ソース装置から受信側のシンク装置にデータキーKseedが安全に送信される。次に、ソース装置は、Kseed

、Secret A及びSecret Bを用いて、モードAの暗号化キーA及びモードBの暗号化キーBを生成する。具体的には、次の式を用いて算出される。

$$\text{KeyA} = h(\text{Kseed} \parallel \text{SecretA})$$

$$\text{KeyB} = h(\text{Kseed} \parallel \text{SecretB})$$

ここで、hはハッシュ関数を表しており、記号a ∥ bは、aとbのビット接続を表している。

【 0 0 6 3 】

ソース装置は、送信されてくるデータに加えられているCCIの値を読む。CCIがコピー禁止を示しているとき、データパケットは、CCIと共に、モードAの暗号キーAによって暗号化される。EMIモード(「11」)がEMIフィールド210に格納され、データパケットがIEEE1994インタフェースを介して送信される。CCIが一世代コピーの許可を示しているとき、データは、CCIと共に、モードBの暗号キーBによって暗号化され、EMIモード(「10」)がEMIフィールド210に格納されてパケット化され、そのパケットがIEEE1994インタフェースを介して送信される。CCIが無制限コピーを示しているとき、データパケットは、暗号化されず、パケット化される。EMIモードが「00」としてEMIフィールド210に格納され、そのパケットが送信される。したがって、データを暗号化するのに送信装置がどのキーを用いるかは、サービスによって決まるのではなく、データに加えられているEMIモードによって決まる。

【 0 0 6 4 】

ソース装置と同様に、シンク装置は、Kseed、Secret A及びSecret BからキーA及びキーBを生成する。受信されたパケットのEMIが、シンク装置によって調べられ、EMIモードがモードAを示すとき、キーAを用いてデータが暗号解読され、EMIモードがモードBを示すとき、キーBを用いてデータが暗号解読される。次に、暗号解読されたデータに加えられたEMIモードが調べられる。EMIモードがコピー禁止を示しているとき、データは記録されない。EMIモードが一世代コピーの許可を示しているとき、EMIモードはコピー禁止に変えられて、データと共に記録される。EMIモードが無制限コピ

ーを示しているとき、データと共に記録される。

【0065】

次に、送信装置が分類Aの装置であり、受信装置が分類Dの装置であるときの処理を説明する。上述した処理のように、ソース装置はシンク装置にK seedを安全に送信する。なお、ここで用いられる秘密コードは、Secret 2T及びSecret 2Rである。ソース装置は、上述したように、キーA及びキーBを生成し、データに加えられたEMIモードに従ってデータを暗号化する。ソース装置はデータパケットに適切なEMIを格納し、それを送信する。

【0066】

シンク装置は、ソース装置と同様の方法で、キーBを生成する。シンク装置が、ライセンスの条件により受信の際にモードAの使用が禁止されており、キーAを生成できない場合を想定する。シンク装置は、受信されたパケットのEMIモードを調べる。EMIモードがモードAであるとき、シンク装置はそのパケットを破棄する。EMIモードがモードBを示しているとき、シンク装置はキーBを用いてデータを暗号解読し、そのパケットを記録する。このとき、データがモードBによって暗号化されたことを示す情報が、データと共に記録される。EMIモードが00を示しているとき、シンク装置はそのままデータを記録する。このとき、データが暗号化されなかったことを示す情報が、データと共に記録される。

【0067】

本発明の好ましい実施の形態である、ソース装置とビットストリーム記録(BSR)装置との間でコピー保護情報を安全に送信するための方法及びシステムが説明されている。本発明は具体的な実施の形態で説明されたが、本発明は、このような実施の形態に限定されると考えられるべきではなく、むしろ、以下の請求の範囲に従って考えられるべきである。

【図面の簡単な説明】

【図1】

FIG. 1は、従来技術のコピー制御情報(CCI)のインタフェースにおける情報パケット中のフィールドの構成を示す図である。

【 図 2 】

FIG. 2 は、ソース装置とシンク装置を備え、不当な妨害装置がその間に接続されている従来技術のシステムの構成を示すブロック図である。

【 図 3 】

FIG. 3 は、ソース装置とシンク装置が接続し、情報パケットの通信を行う、本発明を適用したシステムの構成を示すブロック図である。

【 図 4 】

FIG. 4 は、本発明を適用した略号化モード識別子 (E M I) を含む情報パケット中のフィールドを示す図である。

【 図 5 】

FIG. 5 A は、本発明の第 1 の実施の形態におけるソース装置とこれに接続したシンク装置の具体的な構成を示す回路図である。

【 図 6 】

FIG. 5 B は、本発明の第 2 の実施の形態におけるソース装置とこれに接続したシンク装置の具体的な構成を示す回路図である。

【 図 7 】

FIG. 6 A は、本発明の第 1 の実施の形態の他の実施例におけるビットストリーム記録装置の具体的な構成を示す回路図である。

【 図 8 】

FIG. 6 B は、本発明の第 2 の実施の形態の他の実施例におけるビットストリーム記録装置の具体的な構成を示す回路図である。

【 図 9 】

FIG. 7 は、本発明を適用したソース装置とシンク装置によって行われる処理を示すフローチャートである。

【 図 10 】

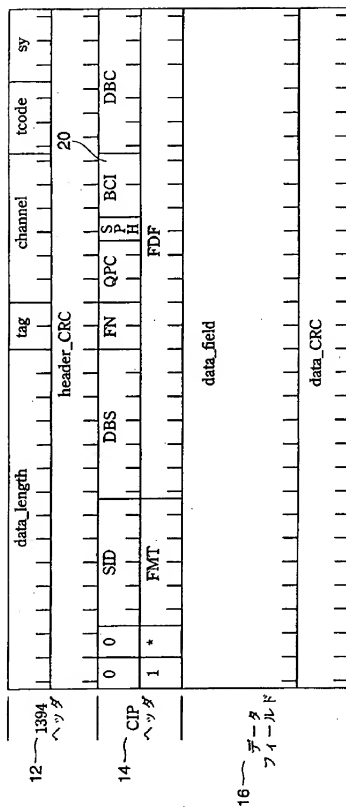
FIG. 8 は、本発明によってサポートされる異なる種類の音声／画像装置と、これらの装置の入力及び出力信号によって用いられる様々な通信モードを示す図である。

【 図 11 】

FIG. 9は、本発明における動作モードを示す図である。

【 図 1 】

10



*: Form_1 (ENC)

FIGURE 1

【 図 2 】

30

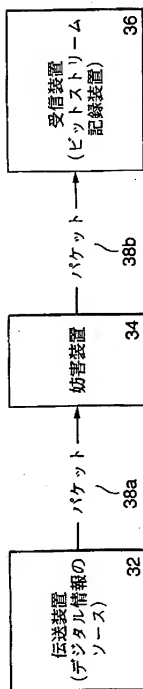


FIGURE 2
(従来技術)

【 図 3 】

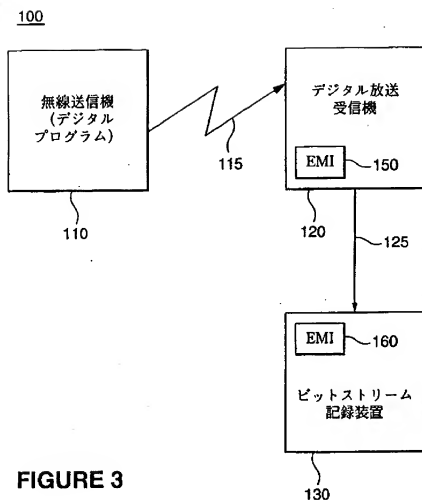
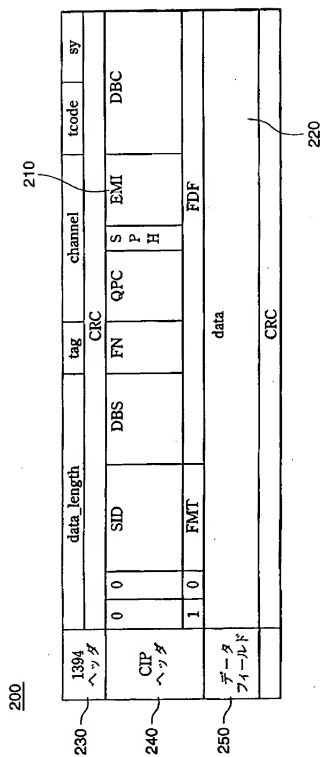


FIGURE 3

【 図 4 】



【図 5】

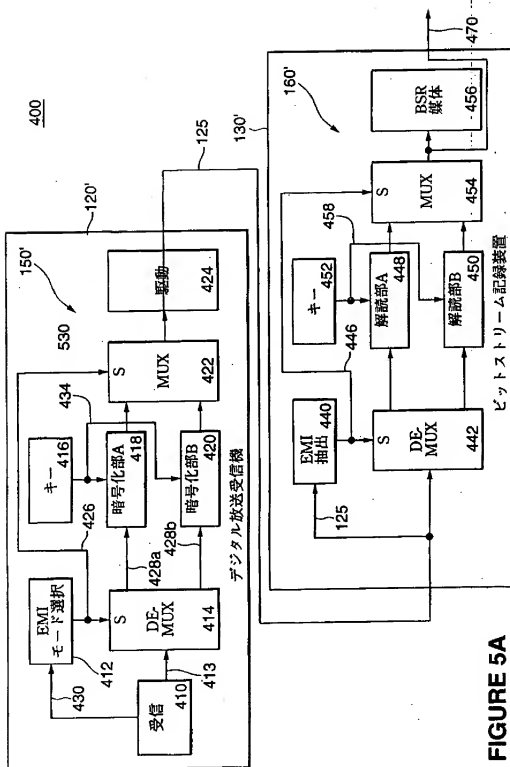


FIGURE 5A

【図 6】

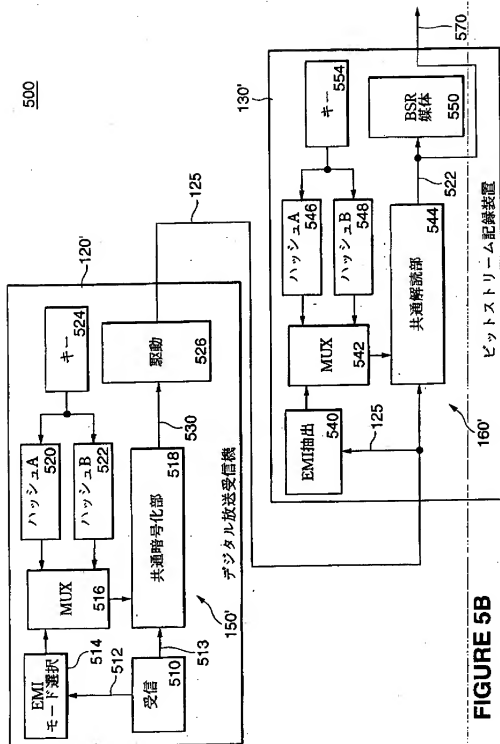


FIGURE 5B

【 図 7 】

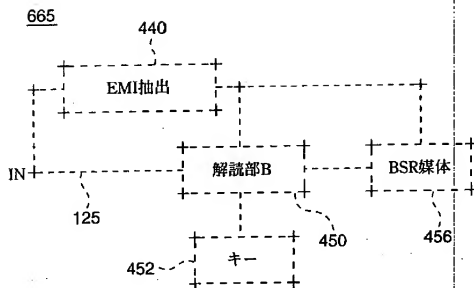


FIGURE 6A

【 図 8 】

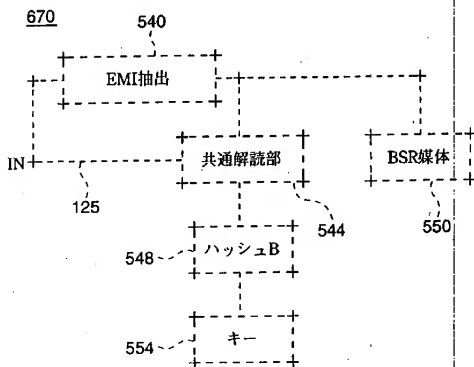


FIGURE 6B

【 図 9 】

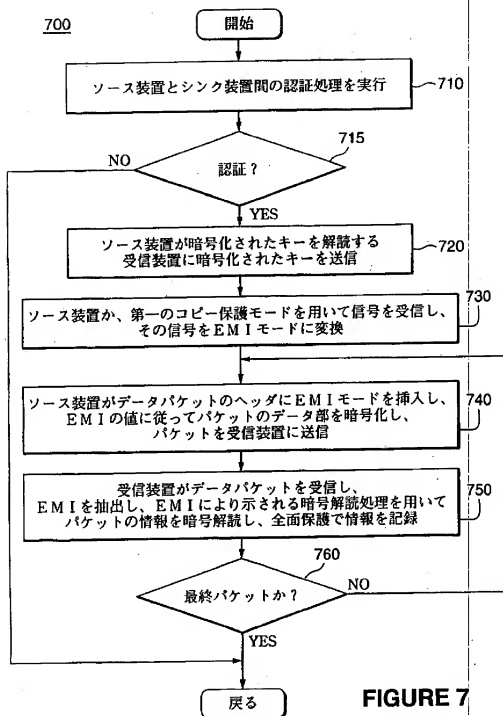


FIGURE 7

【図 10】

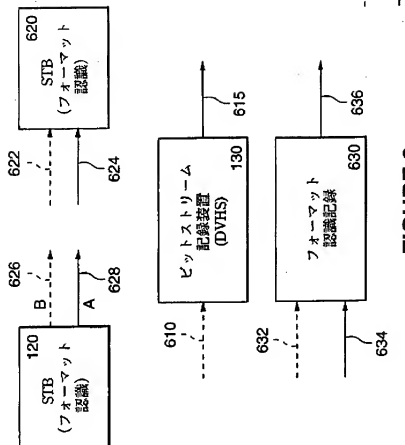


FIGURE 8

【図 11】

300

サービス 1 310	送信 315	SECRET1T
	受信 317	SECRET1R
サービス 2 320	送信 325	SECRET2T
	受信 327	SECRET2R
サービス 3 330	送信 335	SECRET3T
	受信 337	SECRET3R
340 モード A		SECRET A
350 モード B		SECRET B

FIGURE 9

【 国際調査報告 】

INTERNATIONAL SEARCH REPORT

4. CLASSIFICATION OF SUBJECT MATTER IPC 6 G11B20/00 H04N5/913		International Application No. PCT/US 98/22126
According to International Patent Classification (IPC) or to both national classification and IPC		
5. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 G11B H04N		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data bases consulted during the international search phase of data bases and, where practical, search terms used		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 766 466 A (SONY CORP) 2 April 1997 see page 6, line 1 - line 44; figure 9	1,2,4-6, 9
Y	EP 0 691 787 A (SONY CORP) 10 January 1996 see the whole document	1,2,4-6, 9
A	EP 0 763 936 A (LG ELECTRONICS INC) 19 March 1997	
A	WO 97 21279 A (SOLANA TECHNOLOGY DEV CORP) 12 June 1997	
A	US 4 598 283 A (YARBROUGH CHARLES J ET AL) 1 July 1986	
A	EP 0 618 723 A (SONY CORP) 5 October 1994	
-/-		
<input checked="" type="checkbox"/> X	Further documents are listed in the continuation of box C	<input checked="" type="checkbox"/> K Patent family members are listed in annex
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claims or which is cited to establish the publication date of another document or other access reason (as specified)</p> <p>"O" document relating to an oral disclosure, use, exhibition or other practice</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"Z" document member of the same patent family</p>		
Date of the actual completion of the international search		Date of mailing of the international search report
17 February 1999		24/02/1999
Name and mailing address of the ISA European Patent Office, P.O. Box 5016 Palenstein 2 1A, 2520 HD Rijswijk Tel. (+31-70) 540-2040, Tx. 31 051 400 NL Fax. (+31-70) 540-2010		Authorized officer Devergnanne, C

Form PCT/ISA219 (Revised March 1997)

INTERNATIONAL SEARCH REPORT

b. national Application No.
PCT/US 98/22126

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category ¹	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
E	EP 0 878 794 A (SONY CORP) 18 November 1998 see claims 1-7; figures 1-3	11-16

Form PCT/ISAC/10 (continuation of form PCT/ISAC/10 July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Serial Application No.

PCT/US 98/22126

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0766466 A	02-04-1997	JP 9098375 A	08-04-1997
		AU 6580796 A	10-04-1997
		BR 9603952 A	09-06-1998
		CA 2186418 A	30-03-1997
EP 0691787 A	10-01-1996	CN 1115150 A	17-01-1996
		JP 8077706 A	22-03-1996
		US 5796628 A	18-08-1998
EP 0763936 A	19-03-1997	CN 1150738 A	28-05-1997
		JP 9093561 A	04-04-1997
		US 5799081 A	25-08-1998
WO 9721279 A	12-06-1997	US 5719937 A	17-02-1998
		AU 1128397 A	27-06-1997
		EP 0873597 A	28-10-1998
US 4598288 A	01-07-1986	AU 536261 B	03-05-1984
		US 4305101 A	08-12-1981
		AU 6441180 A	20-05-1982
		CA 1159551 A	27-12-1983
		DE 3014309 A	06-11-1980
		FR 2454736 A	14-11-1980
		GB 2046967 A,B	19-11-1980
		JP 55141876 A	06-11-1984
EP 0618723 A	05-10-1994	JP 6339110 A	06-12-1994
		CA 2120360 A	03-10-1994
EP 0878794 A	18-11-1998	JP 10322648 A	04-12-1998
		CA 2236367 A	14-11-1998

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW

(72)発明者 嶋 久登

アメリカ合衆国 カリフォルニア州
95070 サラトガ パセオ フロレス
12510

(72)発明者 浅野 智之

日本国神奈川県横浜市中区 1-15-19-
202

Fターム(参考) 5C053 FA13 FA20 FA22 GB06 GB11
LA15
5D044 AB05 AB07 DE17 DE50 GK17
HL08

【要約の続き】

モードによって異なる暗号化処理を行うことによって、選択される暗号解読処理は、行われた暗号化処理とは異なるため、ソース装置とシンク装置との間に位置してEMIコードを変更する不当な装置は、音声／画像作品をその後再生したり記録したりすることはできない。